Katten

Health Care Law Perspectives

AUGUST 2020 • VOLUME 2

Corona Viruses and Computer Viruses: It's Time for a Cyber Health Check-Up

AUTHORS

MEGAN HARDIMAN DORON GOLDSTEIN JEREMY MERKEL

The health care industry has long been a primary target of malicious cyber criminals, but since the emergence of COVID-19, organizations on the front lines of fighting the pandemic have experienced a rise in cybersecurity incidents and attacks. Between February and June of 2020, HIPAA-covered entities reported 192 large scale data breaches to the US Department of Health and Human Services, Office of Civil Rights (OCR) – more than twice as many as were reported during the same period in 2019.[1]

While the types of cyber threats health care organizations have encountered during the COVID-19 pandemic are not wholly original, factors including the rapid shift to remote work, the expansion of telehealth and the strain on resources experienced by many organizations, have combined to create new security vulnerabilities and challenges. For example, in recent months, some health care organizations may have temporarily relaxed firewall rules to facilitate additional work-from-home capabilities, short-circuited vendor diligence or contracting protocols in order to rapidly deploy or expand telehealth capabilities, or quickly erected temporary medical facilities in parking lots and convention halls that lacked traditional security infrastructure. While governmental authorities have (temporarily) waived various regulatory standards and eased enforcement for certain privacy, security and breach notification requirements during the public health emergency, malicious cyber actors cannot be expected to show similar restraint.

The Evolving COVID-19 Cyber Threat Landscape

While the types of cyber threats health care organizations have encountered during the COVID-19 pandemic are largely similar to the pre-COVID landscape, cyber threat actors are exploiting pandemic-related fear and uncertainty, as well as new vulnerabilities created by the shift to virtual environments. The FBI's Internet Crime Complaint Center (IC3) reported that it had received 1,200 complaints related

[1] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. U.S. Department of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited June 29, 2020).

IN CASE YOU MISSED IT

Coronavirus (COVID-19) Resource Center

As the coronavirus (COVID-19) continues to impact our world, stay up to date on Katten's Coronavirus Resource Center. The latest legal news by topic area, firm event information and more will be featured as it is released.

SAMHSA Finalizes Interim Changes to Substance Use Disorder Confidentiality Rule Pending Implementation of Deeper CARES Act Reforms

Katten attorneys breakdown the SAMHSA interim rule on privacy protections for patient records related to federally assisted substance abuse programs, while anticipating more changes to come as a result of the CARES Act.

Governing Technology in Times of Crisis

Doron Goldstein contributed to *ITechLaw* and the Human Technology Foundation's report on the technological, ethical and legal implications of deploying COVID-19 contract tracing technologies.

Coronavirus (COVID-19) Federal and New York Health Care Primary Legal Sources

Joseph Willey and the Health Care team have developed a resource guide with links to the latest guidance coming out of the federal government, the State of New York, New York City and other pertinent health care-related entities.

to coronavirus cyber threats through March, which far surpasses the number of complaints it received for all types of internet fraud in 2019.[2] Authorities have warned that cyber actors are targeting health care bodies, pharmaceutical companies, academia, medical research organizations, and local governments, as well as others involved in the national pandemic response. In addition to seeking to steal information for commercial gain, hackers may attempt to steal valuable information related to the pandemic response strategy, such as sensitive COVID-19-related research or intelligence on national and international healthcare policy.

The sophisticated threat actors that are exploiting the COVID-19 crisis have a global reach. In March, Canada's Centre for Cybersecurity warned of malicious hackers targeting their health care sector to gain unauthorized access to intellectual property and research and development related to COVID-19. Simultaneously, the Czech Republic faced a series of cybersecurity incidents, including an attack against one of its largest COVID-19 testing facilities, which caused it to terminate operations and relocate patients to other hospitals. The danger to public health and safety resulting from such malicious activity prompted the U.S. Department of State to condemn this cyber warfare in a call for global action.[3]

Below are a few examples of cyber threats in the era of COVID-19, as well as some practical steps organizations can take to manage cyber risk in today's increasingly virtual environment.

Ransomware Threats Targeting Health Care Organizations

In the early stages of the pandemic, hacking groups pledged to spare hospitals and health care organizations from cyberattacks. These "assurances" were short lived. In March, hackers deployed the ransomware variant known as *Maze* to attack a U.K.-based laboratory that was testing COVID vaccines. *Maze* has the ability to exfiltrate files on a system, and pressures the victim to pay a ransom by threatening to publish the data on the dark web. Fortunately, the facility was able to restore their systems, but that didn't stop the hackers from pressuring them to pay the ransom by publishing thousands of patient records containing medical questionnaires and copies of passports on the Internet (reportedly, the facility never paid).[4] In June, the University of California San Francisco reported that it paid a $1.14 million ransom after malware encrypted certain servers within its school of medicine.[5]

In response to the continued threat of ransomware attacks targeting the health care sector, Microsoft's Threat Protection Intelligence Team warned hospitals that their network devices and VPNs were specific targets as organization transitioned to a remote workforce.[6] The warning was consistent with a joint

[2] *Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments*. Federal Bureau of Investigation, https://www.ic3.gov/media/2020/200401.aspx (April 1, 2020).

[3] *The United States Concerned by Threat of Cyber Attack Against the Czech Republic's Healthcare Sector.* US Department of State, https://www.state.gov/the-united-states-concerned-by-threat-of-cyber-attack-against-the-czech-republics-healthcare-sector/ (April 17, 2020).

[4] *COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online. Forbes*, https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/#78b40ab218e5 (March 23, 2020).

[5] *Update of IT Security Incident at UCSF.* https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf (June 26, 2020).

Coronavirus (COVID-19) Federal and Illinois Health Care Primary Legal Sources

Katten's Health Care team has developed a resource guide with links to the latest guidance coming out of the federal government, the State of Illinois, the City of Chicago and other pertinent health care-related entities.

Governor Issues Guidance on Reopening for Texas Health Care Providers

Kenya Woodruff and Michelle Apodaca have developed the following resource guide with links to the Texas Governor Greg Abbott's latest orders.

COVID-19 Considerations for Employers

Katten's Employment Litigation and Counseling attorneys explored the key considerations for employers confronting challenges related to leaves of absence, layoffs, workplace safety, employee conduct policies, remote work and more.

CARES Act Provider Relief Fund: FAQs

The US Department of Health and Human Resources maintains and frequently updates its Provider Relief Fund FAQs, available via its Coronavirus portal.

New State Appellate Court Interpretation of the Patient Safety Act Privilege Protections

On June 3, Michael Callahan published an advisory on the new appellate court decision in Pennsylvania interpreting the scope of privilege protections under the Patient Safety Act and Pennsylvania's Peer Review Protection Act (PRPA).

OCR Fine Calls Attention to HIPAA Security Rule Compliance

Megan Hardiman and Cheryl Camin Murray published an advisory on March 10, highlighting best practices for risk management while adhering to HIPAA security rule requirements.

alert issued by the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI on May 22, in which the agencies reported that unpatched VPNs topped the list of vulnerabilities being routinely exploited by sophisticated foreign cyber actors in 2020.[7] The *REvil* (a.k.a. *Sodinokibi*) variant is one of the ransomware campaigns that actively exploits these vulnerabilities to penetrate an organization's infrastructure. Following a successful exploitation, the hackers can steal credentials, elevate privileges and move laterally across compromised networks, installing ransomware or other malware payloads. In contrast to auto-spreading ransomware, like *WannaCry* or *NotPeya*, in which hackers employ credential theft and lateral movement methods traditionally associated with nation-state actors, *Maze* and *REvil* are human-operated ransomware campaigns, which incorporate social engineering tactics that exploit users' fears and need for information. This is why the hackers behind these types of ransomware target organizations that are most vulnerable to disruption, like those that have not had the time or resources to assess security hygiene, install the latest patches, update firewalls, or check the privilege levels of users and endpoints. In the age of COVID-19, health care organizations may be particularly vulnerable.

COVID-Related Phishing Attacks and Voicemail Phishing

Bad actors carrying out email phishing attacks have exploited fears about the coronavirus and relied on impersonation tactics, like spoofing communications from governmental agencies like the Center for Disease Control or World Health Organization to induce users to enter credentials or click links that install malware and put sensitive and confidential information at risk. According to Bitdefender, hospitals and clinics, pharmaceutical institutions, and distributors of medical equipment are the most frequent targets of phishing email campaigns, with messages about COVID treatments and therapies, or personal protective equipment (PPE) that is in low supply.[8] In fact, American, Canadian and British organizations that are rushing to develop a coronavirus vaccine have been targeted by Russian cyber criminals aimed at stealing research and medical supply chain data in order to win the race for a vaccine. According to the National Security Agency, the hackers responsible for this espionage are known as APT29 and Cozy Bear, which are the same groups associated with hacking the Democratic National Committee's servers during the 2016 election.[9]

Another phishing method is voicemail phishing. Some health care organization are using legacy phone systems known as Private Branch Exchange (PBX) to automate calls and record voicemail messages that are sent to users' inboxes so employees don't miss important messages while working remotely.[10] The scheme involves the attackers spoofing messages from the PBX system and informing an employee that they have a new voicemail message. To hear the message, the user is directed to a website that spoofs PBX integrations with the aim of stealing credentials. The hackers rely on the fact that users have the same access credentials across multiple platforms, which may contain personal or proprietary information.

Password Spraying (and Credential Stuffing) Directed at Health Care Organizations

Password spraying is a type of brute-force attack in which hackers try to obtain the passwords of multiple accounts at once by feeding many usernames or email addresses into a program that attempts to match those accounts with commonly used passwords. A joint advisory issued by CISA and the UK's National Cyber Security Centre (NCSC) warned of this threat being directed at health care and medical organizations, and advised users to change any passwords that could be reasonably guessed to one created with three random words.[11]

---

[6] *Microsoft works with healthcare organizations to protect from popular ransomware during COVID-19 crisis: Here's what to do.* https://www.microsoft.com/security/blog/2020/04/01/microsoft-works-with-healthcare-organizations-to-protect-from-popular-ransomware-during-covid-19-crisis-heres-what-to-do/ (April 1, 2020).

[7] *Top 10 Routinely Exploited Vulnerabilities*. US Department of Homeland Security, https://www.us-cert.gov/ncas/alerts/aa20-133a (May 12, 2020).

[8] *5 Times More Coronavirus-themed Malware Reports during March*. Bitdefender, https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/ (March 20, 2020).

[9] *Russia Is Trying to Steal Virus Vaccine Data, Western Nations Say. New York Times*, https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html?searchResultPosition=5 (July 16, 2020).

[10] *Voicemail Phishing Scam Identified Targeting Remote Healthcare Workers. HIPAA Journal*, https://www.hipaajournal.com/voicemail-phishing-scam-identified-targeting-remote-healthcare-workers/ (June 8, 2020).

[11] *APT Groups Target Healthcare and Essential Services*. US Department of Homeland Security, https://www.us-cert.gov/ncas/alerts/AA20126A (May 5, 2020).

Similarly, credential stuffing involves the automated injection of usernames and password combinations that have previously been compromised, usually in an older data breach, to gain access to user accounts. In April, over 500,000 Zoom account credentials that were gathered through credential stuffing were sold on dark web for less than a penny, and in some cases, were given away for free.[12] The consequences of this have been seen through the rise of "Zoom-bombing" and other malicious activity involving video-teleconferencing platforms.[13] To reduce the risk of these types of attacks, organizations are strongly encouraged to implement multi-factor authentication and require that employees change their passwords frequently.

Tips for Better Cyber Health

- **Update your security risk analysis and risk management plans.** Ensure your security risk analysis is updated for technology and operational changes made in response to the pandemic and implement any corresponding risk treatment plans to reduce the likelihood of being impacted by a cybersecurity incident, such as a ransomware attack. In particular, be sure to identify potential risks and vulnerabilities related to expanded remote work, deployment of new telehealth capabilities and technologies and development of additional testing and treatment locations.
- **Confirm full compliance of telehealth operations.** Providers that rolled out telehealth services in a manner that may not have fully complied with HIPAA standards in reliance on OCR's Notice of Enforcement Discretion and/or other temporary waivers of privacy/security requirements should ensure that they have, at a minimum, implemented all recommendations set forth in the Notice (for example, enabling all available encryption and privacy settings, providing notification to patients that of potential privacy risks, entering into appropriate business associate agreement with the technology vendor).[14] In accordance with the US Department of Health and Human Services' guidelines of voluntary cybersecurity practices for health care organizations, providers should also identify any HIPAA and other privacy and security law gaps, and develop a plan to remediate any vulnerabilities as soon as possible.[15]
- **Review privacy and security policies and procedures.** Review, and if necessary expand, your privacy and security policies and procedures to be sure they adequately address current operations, particularly in regards to remote work, telehealth and any other new or expanded operations. More information from Katten on best practices for remote work is available here.
- **Update training to reflect the current environment.** To ensure personnel are aware of their privacy and security obligations in the COVID era, train regularly on your policies and post the policies on the organization's intranet and/or circulate them to personnel via email. Training should be practical and reflect today's virtual environment – from using secure collaboration tools, to identifying COVID phishing emails and scams, to securely disposing of paper when working from home.

Katten's Health Care and Privacy, Data and Cybersecurity teams continue to monitor the COVID-related cyber threats, and is standing by to advise on the precautions that health care organizations can take to reduce the risk of being impacted by a cybersecurity incident.

---

[12] *Zoom Gets Stuffed: Here's How Hackers Got Hold Of 500,000 Passwords. Forbes*, https://www.forbes.com/sites/daveywinder/2020/04/28/zoom-gets-stuffed-heres-how-hackers-got-hold-of-500000-passwords/#4768c0cb5cdc (April 28, 2020).

[13] *FBI Releases Guidance on Defending Against VTC Hijacking and Zoom-bombing*. Federal Bureau of Investigation, https://us-cert.cisa.gov/ncas/current-activity/2020/04/02/fbi-releases-guidance-defending-against-vtc-hijacking-and-zoom (April 2, 2020).

[14] *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency*. US Department of Health and Human Services, Office for Civil Rights, https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html (March 30, 2020).

[15] *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*. US Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Response, https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf (last visited July 14, 2020).

Physician Late Career Policies Under EEOC Attack[1]

AUTHOR | CONTRIBUTOR


MICHAEL R. CALLAHAN ASHLEY OGEDEGBE

What do commercial pilots, FBI agents and air traffic controllers have in common? These individuals all face mandatory retirement ages.[2] The Association of American Medical Colleges concluded that one-third of practicing physicians are 65 or older,[3] but unlike other industries, there is currently no mandatory retirement age for physicians. Some hospitals and medical staffs have begun implementing policies known as, "Late Career Practitioner Policies," to detect the presence of physical, psychological or cognitive deficiencies that may affect a physician's ability to practice medicine consistent with acceptable standards of care. But critics question whether these policies subject older physicians to discriminatory scrutiny.

Risk vs. Reward: Evaluating the Risks and Benefits of Aging Practitioners

Physicians are not immune from the vicissitudes that come with aging. Numerous studies demonstrate that aging can negatively impact cognition, judgment, and physical senses such as sight and hearing.[4] But for every study that discusses the pitfalls of aging physicians, there is another study that praises aging physicians.[5] Older physicians can provide invaluable training and mentoring to younger physicians, and some studies indicate that older physicians may actually make less errors than younger, less experienced physicians. Due to the conflicting literature, some say there is insufficient data to support the policies. But are they correct?

Are Late Career Practitioner Policies Responsible or Discriminatory?

Some hospital systems and providers attempt to mitigate the risk of adverse events from aging physicians by adopting late career practitioner policies. But providers who choose to adopt the policies may also risk violating the following statutes:

- **Age Discrimination in Employment Act[6] (ADEA).** The ADEA makes it unlawful, among other things, for an employer to:
  - Fail or refuse to hire or to discharge any individual or otherwise discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's age; and
  - Limit, segregate or classify his employees in any way which would deprive or intend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual's age.

---

1 Article adapted from a May 12, 2020 presentation by Michael R. Callahan, Esq. of Katten and Carol S. Cairns, CPMSM, CPCS, President of PRO-CON. ("Presentation")

2 Congress has approved fixed retirement ages for certain industries that affect public safety. *See* 49 U.S.C. § 44729 (mandating retirement for commercial airline pilots at age 65); *see also* Public Law 101-509 (mandating retirement for FBI agents at age 57); *see also* Public Law 92-297 (mandating retirement for air traffic controllers at age 56).

3 AAMC, *New Findings Confirm Predictions on Physician Shortage*, Apr. 23, 2019.

4 Douglas H. Powell, *Profiles in Cognitive Aging* (1994) (explaining declining mental functions associated with aging); Grace ES, Wenghofer EF, Korinek, EJ, *Predictors of physician performance on competence assessment: Findings from CPEP*, The Center for Personalized Education for Physicians (2014) (finding older physicians were more likely to provide unsafe outcomes); American Medical Association, *Report 5 of Council on Medical Education Competency and the Aging Physician* (2015) (identifying factors that affect clinical performance).

5 Roger Collier, *Diagnosing the Aging Physician*, CMAJ, Apr. 22, 2008 (quoting Kevin Eva, *The Aging Physician: Changes in Cognitive Processing and Their Impact on Medical Practice*, Acad. Med., Oct. 2002 (finding "older doctors are superior at particular tasks, such as making initial diagnoses").

6 Age Discrimination in Employment Act of 1967, 29 USC § 621, et. seq.

- **Americans with Disabilities Act[7] (ADA).** The ADA states that an employer "shall not require a medical examination and shall not make inquiries of an employee as to whether such employee is an individual with a disability or as to the nature or severity of the disability, unless such examination or inquiry is shown to be job-related and consistent with business necessity."[8]

A recent example provides insight regarding how regulators view these policies. On February 9, the Equal Employment Opportunity Commission (EEOC) filed a complaint against Yale New Haven Hospital (Hospital).[9] The complaint was filed after a complaint brought by a pathologist and class of older physicians who alleged that the Hospital's policy violated the ADEA and the ADA to the EEOC failed to be successfully conciliated.

As background, the medical staff physicians were not employees of the Hospital, but rather employees of Yale Medical School (YMS). An affiliation agreement between the Hospital and YMS fully integrated their operations, and all YMS faculty with clinical department appointments were required to obtain medical staff privileges at the Hospital.

In March 2016, the Hospital adopted a policy that mandated neuropsychological and ophthalmologic screening exams for all medical staff ages 70 or older. The screenings focused on evaluating the cognitive function of the individuals by measuring items such as information processing, memory and concentration levels, and psychomotor efficiency. A medical staff committee reviewed the physicians' medical results and made recommendations to the Credentials Committee based on the results. Physicians were graded on a scale that ranged from: "Passed, Qualified Passed, Borderline Deficient, Deficient, or Failed." When Yale applied the policy in April 2019 against 145 individuals ranging from ages 70 to 84: 80 Passed, 38 Qualified Passed, 14 individuals were "Borderline Deficient," one was "Deficient," and seven "Failed." Of those who were retested, a number of them resigned and others were placed under additional scrutiny.

The EEOC argued that the Hospital's policy violated the ADEA by subjecting practitioners age 70 and above to unlawful and willful discrimination and classification. Moreover, the EEOC argued that the policy deprived the practitioners of their right to equal employment practices. The EEOC also asserted that the Hospital violated the ADA by interfering with the practitioners' right to enjoy employment free from unlawful medical examinations.

Another issue is whether the physicians can be treated as Hospital employees based on certain control factors even though they are otherwise independent contractors. An alternative theory which the EEOC is asserting is that the Hospital will qualify as a covered third-party employer. Employers and covered third-party employers are prohibited from discriminatorily interfering with an individual's employment opportunities.[10] Here, the class of physicians are employed by YMS, not the Hospital who implemented the policy. The EEOC argued that the Physicians should be treated as Hospital employees based on the affiliation agreement. But even without an agreement, a claimant can establish an employment relationship by showing that the employer has sufficient and direct control over the individual.[11] The EEOC is not yet required to prove the basis of its claims and must point to evidence that demonstrates that the Hospital had sufficient control over the physicians.[12]

---

7 Americans with Disabilities Act of 1990, 42 USC § 12101, et. seq., as amended by the Americans with Disabilities Act Amendment Act of 2008.

8 *Id*.

9 *See* EEOC v. Yale New Haven Hospital, Civil Action No. 3:20-cv-00187; *see also* EEOC, https://www.eeoc.gov/newsroom/eeoc-sues-yale-new-haven-hospital-age-and-disability-discrimination.

10 Jeffrey R. Pittman, *Employment Law for Business*, at 129 (2013) (explaining third-party interference can exist even where an employment relationship has never existed between a third-party employer and an individual).

11 Some factors include to show that an employer has sufficient control over an individual to establish an employer-employee relationship include: controlling when, where, and how the individual performs the task; if the task requires a high level of skill or expertise; providing supplies to the individual; setting the schedule of the hours and duration of the task; and paying an hourly, weekly, or monthly wage rather than by task.

12 Def.'s Answer to Pls.' Compl. *EEOC v. Yale New Haven Hospital, Civil Action No. 3:20-cv-00187*.

Should Providers Implement Late Career Practitioner Policies?

The recent EEOC complaint against Yale may serve as a warning for healthcare providers who decide to implement late career practitioner policies solely based on age. Providers seeking to implement these policies should seek legal counsel to determine whether its physicians will be treated as employees or independent contractors for purposes of Title VII, the ADEA or the ADA.

Other ways which providers currently oblige to ensure that patient safety through age neutral policies include the following:

- **Code of Conduct and/or Disruptive Behavior Policies;**
- **FPPE/OPPE Policies.** Identify department-specific criteria to evaluate physicians on an ongoing and neutral basis. In addition to established criteria, the hospital can include several identified factors associated with aging and physical, psychological and cognitive decline irrespective of age and then proceed accordingly[13];
- **Physician Wellness Committees.** Designate a multidisciplinary committee to evaluate medical staff for impairments that could result in adverse patient consequences when there is a reasonable suspicion of impairment; and
- **Non-Disciplinary Remedial Measures.** Implement non-disciplinary, remedial steps to prevent adverse events when deficits are identified in lieu of restricting or terminating privileges such as encouraging retraining and reeducation, providing or requiring consultations with other physicians for second opinions, and providing memory aides to all physicians.

[13] See Presentation at slides 48-54.

Radiology Business Journal Talks Practice Sales During a Pandemic With W. Kenneth Davis, Jr.


W. KENNETH DAVIS, JR.

Radiology Business Journal spoke with Health Care partner, W. Kenneth Davis, Jr., about radiology practices considering what he described as "existential deals" to be acquired by investor-owned physician practice management companies (PPMCs), particularly in light of the COVID-19 pandemic. The article was featured in *Radiology Business's* e-newsletter and the *Radiology Business Journal* magazine. Maintaining his view as a PPMC agnostic, Ken suggested that practices look at the "level of investor involvement" as part of the decision-making process. He noted that there are two main categories of acquirers: "radiology-focused PPMCs run by radiologists who commonly work in partnership with finance firms" and "multispecialty PPMCs whose interests include but aren't exclusive to radiology."

Depending on practice size and complexity, Ken stated that often radiologists first "look at the infrastructure their practices need in order to grow — PACS, RIS, EHR, revenue cycle management functions — and ask themselves, 'Hey, are we really going to do this on our own? What's it going to cost? Do we truly want to spend millions of dollars on [technology], or are we just better off selling to a PPMC?'" He added that practices must weigh their openness to change. "No PPMC sits down with practice leaders and says, 'Doctors, we're buying your practice, and things are going to change in terms of control.' If you can't accept that change is inevitable, no matter which model you'd be following, then a deal probably isn't the best idea for your practice." Ken also noted that joint ventures with other radiology practices (perhaps even a merger) or membership in a multi-practice alliance could be solid alternatives for practices to consider if a PPMC is not a good fit. ("COVID or Not, Big Money is Buying Radiology Practices. Should Yours Be Selling?," April 29, 2020)

COVID-19 and PREP Act Immunity

AUTHOR

KENYA S. WOODRUFF

In the wake of rising COVID-19 infections, many private companies have donated goods and services, developed testing and diagnostic tests, provided COVID-19 testing support to state and federal governmental entities, and worked to develop antiviral drugs that will be effective against the novel virus. Some of these tests and processes are new and unproven, and the immunities offered by The Public Readiness and Emergency Preparedness Act (PREP Act) are key to their willingness to continue their efforts to support the COVID-19 response. The PREP Act was enacted by Congress and signed into law by George W. Bush in 2005 in the wake of an avian influenza outbreak. Vaccine manufacturers lobbied for this legislation to preempt state vaccine safety laws in the case of an emergency declaration by the US Department of Health and Human Services (HHS).

The PREP Act authorizes the Secretary of HHS to issue a declaration (PREP Act declaration) that provides immunity from liability (except for willful misconduct) for claims of loss caused by, arising out of, relating to, or resulting from the administration or use of countermeasures to diseases, threats, and conditions determined by the Secretary to constitute a present, or credible risk of a future, public health emergency to entities and individuals involved in the development, manufacture, testing, distribution, administration, and use of such countermeasures. A PREP Act declaration is specifically for the purpose of providing immunity from liability.

PREP Act immunity applies to any "covered person" with respect to all "claims for loss" caused by, arising out of, relating to, or resulting from the "administration" or the "use" of a "covered countermeasure" if a declaration has been issued with respect to that countermeasure.[1]

Relevant PREP Act Statutory Definitions

Covered Persons are individual persons and entities including, at the Secretary's discretion, manufacturers, distributors, program planners (i.e., individuals and entities involved in planning and administering programs for the distribution of countermeasures), and qualified persons who prescribe, administer, or dispense countermeasures (i.e., healthcare and other providers). The US officials, agents and employees of any of these entities or persons are also covered persons.[2]

Activities Covered are the development, manufacture, testing, distribution, administration and use of countermeasures.[3]

Countermeasures Covered include vaccines, drugs or medical devices to be used against chemical, biological, radiological and nuclear agents of terrorism, epidemics and pandemics.[4]

Claims for Loss are claims from tort liability except for willful misconduct. PREP Act immunity covers death and physical, mental or emotional injury, illness or disability, and the fear of these conditions. Liability protections also extend to claims made for medical monitoring as well as loss or damage to property, including business interruption. Claims that have a connection to the development, distribution, administration or use of the covered countermeasure are also potentially included within the scope of PREP Act liability protections.[5]

---

1 42 U.S.C. § 247d-6d(a)(1).

2 *Id.* at (i)(2).

3 *Id.* at (i)(8).

4 *Id.* at (i)(1)(7).

5 *Id.* at (c)(3).

Limitations

Immunity from liability under the PREP Act is not available for death or serious physical injury caused by willful misconduct. A "serious physical injury" is one that is life-threatening, or results in or requires medical or surgical intervention to preclude permanent impairment of a body function or results in permanent damage to a body structure. Willful misconduct is misconduct that is greater than any form of recklessness or negligence. It is defined in the PREP Act as an act or failure to act that is taken: 1) intentionally to achieve a wrongful purpose; 2) knowingly without legal or factual justification; and 3) in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit. All three of these conditions must be proven with clear and convincing evidence.[6] Willful misconduct cannot be found against:

- a manufacturer or distributor for actions regulated by HHS under the Public Health Service Act or the Federal Food, Drug and Cosmetic Act, if HHS chooses not to take an enforcement action against the manufacturer or distributor, or if HHS terminates or settles an enforcement action without imposing a criminal, civil, or administrative penalty;[7] or
- a program planner or qualified person who acts in accordance with applicable directions, guidelines or recommendations issued by HHS regarding administration and use of a countermeasure as long as HHS or the State or local health authority is notified about the serious injury or death within seven days of its discovery.[8]

Litigation

There are very few reported cases interpreting the PREP Act. The cases below, however, provide insight as to the way in which the PREP Act immunities are applied on the state and federal levels.

In *Parker v. St. Lawrence City Public Health Department*,[9] a parent of a kindergartner who was inoculated for the H1N1 influenza without her parent's consent, filed a lawsuit in New York state court against the health department that administered the vaccine. The Appellate Division of the Supreme Court of New York held that the lawsuit was preempted by the PREP Act and dismissed the case.

In *Kehler v. Hood*,[10] a patient sued his physician and employer in state court for being vaccinated without his informed consent for the H1N1 influenza. The physician and employer then filed a third-party complaint against the vaccine manufacturer. The vaccine manufacturer removed the case to federal court. The federal court held that the PREP Act barred the claims against the vaccine manufacturer. This ruling divested the federal court of jurisdiction to decide the remaining claims against the physician and employer.

Conversely, in *Casabianca v. Mount Sinai Medical Center, Inc.*,[11] a New York state court held that a hospital's failure to inoculate the plaintiff for H1N1 influenza was not a covered countermeasure under the PREP Act because the vaccine was never given. Accordingly, the state court concluded that the PREP Act's immunity provisions did not apply.

---

6 *Id.* at (c)(3).

7 *Id.* at (a)(4).

8 *Id.*

9 102 A.D.3d 140 (2012).

10 2012 WL 1945952 (E.D.Mo.).

11 2014 N.Y. Slip Op. 33583 (N.Y. Sup. Ct. 2014).

COVID-19 Emergency Declaration

On March 10, the Secretary of HHS made a public health emergency declaration for COVID-19, which makes the PREP Act's protections applicable to the COVID-19 pandemic. This declaration was effective February 4 and will continue through October 1, 2024. Under the March 10 declaration, covered countermeasures are any:

> antiviral, any other drug, any biologic, any diagnostic, any other device, or any vaccine, used to treat, diagnose, cure, prevent, or mitigate COVID–19, or the transmission of SARS-CoV–2 or a virus mutating therefrom, or any device used in the administration of any such product, and all components and constituent materials of any such product.[12]

The Advisory Opinion issued by HHS on April 17 and modified on May 19, explained that when considering the terms of the PREP Act and the parameters of the COVID public health declaration in order to meet the definition of a qualified pandemic or epidemic product, a product:

1. must be used for COVID-19; and
2. must be:
    a. approved, licensed, or cleared by Food and Drug Administration (FDA);
    b. authorized under an Emergency Use Authorization issued by the FDA;
    c. described in an Emergency Use Instructions issued by the Centers for Disease Control; or
    d. used under either an Investigational New Drug application or an Investigational Device Exemption.[13]

As private companies continue to develop vaccines, tests and other COVID-19 countermeasures, we expect to see further invocation of PREP Act immunities.

---

[12] 85 Fed. Reg. 15,198,15,202 (March 17, 2020).

[13] US Dep't of Health & Human Services, Advisory Opinion 20-02 (May 19, 2020), *available at*: https://www.hhs.gov/sites/default/files/advisory-opinion-20-02-hhs-ogc-prep-act.pdf.